#7

Attorney's Docket No.: US 1295/01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of		:	June 24, 2002
Catherine A. HAALA		:	
Serial No.:	09/985,734	:	
Filed:	November 6, 2001	:	Group Art Unit: 2131
For:	METHOD AND SYSTEM FOR OBSTRUCTING A PERSON FROM NEGOTIATING A TRANSACTION WITH ANOTHER PERSON, GROUP, OR ENTITY IN A POPULATION	:	**Attn: Pincus Laufer Special Program Examiner**

SUPPLEMENTAL
PETITION FOR ACCELERATED EXAMINATION
UNDER 37 CFR § 1.102 AND MPEP § 708.02(VIII)

Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

In support of her Petition for Accelerated Examination Under 37 CFR § 1.102 and MPEP § 708.02 (VIII) filed on April 26, 2002, Applicant provides a further detailed discussion of the references deemed most closely related to the subject matter encompassed by the claims. In particular, Applicant deems U.S. Patents 6,219,439, 6,213,391, 6,208,264, 4,993,068, and 4,707,592 to be most closely related to the subject matter of the present claims. These references are already of record.

THE INVENTION

The present invention is directed to a method of obstructing a person from negotiating a transaction, including a second or subsequent transaction, with another person, group, or entity in a population, which includes, *inter alia*:

i) comparing the identifying biometric characteristic and the profile information of a person wishing to negotiate a transaction, determined from the portable data device carried by that person, with the corresponding identifying biometric characteristic and the profile information prestored at a central location, for a successful or unsuccessful comparison **(crosscheck)** (see subparagraph f) of Claims 1 and 14),

ii) comparing the identifying biometric characteristic and the profile information determined from the portable data device carried by the person, with the profile information and biometric characteristic obtained directly from the person, for a successful or unsuccessful comparison **(verification)** (see subparagraph h) of Claims 1 and 14), and

iii) determining an active or inactive status of the data device carried by the person **(validation)** (see subparagraph i) of Claims 1 and 14).

The person is obstructed from negotiating the transaction if an unsuccessful comparison is indicated in either steps recited in subparagraphs f) or h), or if the status of the data device is determined to be inactive in the step recited in subparagraph i).

Further, an appropriate authority is notified if the status of the data device is determined to be inactive (see subparagraph k) of Claims 1 and 14).

In summary, the claimed invention requires **verifying** and **crosschecking** the identity of the person, and checking the **status or validity** of the data device carried by the person. If an unsuccessful result is obtained in verification or crosschecking steps, or the data device is determined to be inactive, the person is obstructed from negotiating the transaction. Further, an appropriate authority is notified if the data device is determined to be inactive.

As further recited in Claim 2, the method of the present invention further obstructs the person, obstructed from negotiating an earlier transaction, from negotiating any subsequent transaction with any other person, group, or entity in the population.

As further recited in Claim 3, the method of the present invention notifies a law enforcement authority.

As further recited in Claim 4, the method of the present invention applies to a transaction having a value of at least $100.00.

As further recited in Claim 9, the method of the present invention updates the profile information of the person obstructed from negotiating a transaction, to include details of the transaction, including amount of transaction, identity of the person, group, or entity with whom the transaction was being negotiated by the person, and the category of the transaction.

As further recited in Claim 10, the method of the invention includes further updates the profile information of the person obstructed from negotiating a transaction, to include details of each transaction attempted to be negotiated by the person subsequent to a transaction.

As further recited in Claim 11, the method of the present invention includes converting the data device to an inactive status upon the occurrence of an event, such as expiration of a pre-fixed duration of time (Claim 12).

As further recited in Claim 15, the value of the first transaction is at least $150.00, and the value of the second or subsequent transaction is lower than the value of the first or previous transaction by a predetermined amount, for example, $50.00 (Claim 16).

As recited in Claim 17, the present national security system for obstructing a person from negotiating a transaction with another person, group or entity in a population, includes, *inter alia*:

i) a card reader including a first processing unit for comparing the biometric characteristic stored on the national security card of a person with the biometric characteristic obtained directly from that person for a successful or unsuccessful comparison **(verification)** (see subparagraph d) of Claim 17), and

ii) a remote second processing unit including prestored profile information and an identifying biometric characteristic of each person in a selected section of the population (see subparagraph e) of Claim 17).

One of the first and second processing units compares the profile information and the biometric characteristic stored on the national security card with the profile information and the biometric characteristic prestored on the second processing unit for a successful or unsuccessful comparison **(crosscheck)** (see subparagraph g) of Claim 17).

One of the card reader and the second remote processing unit includes means for determining the active or inactive status of the national security card, and communicating inactive status to a predetermined authority (see subparagraph h) of Claim 17). An inactive status of the national security card obstructs the person from negotiating a transaction with another person, group, or entity in a population.

As further recited in Claim 20, the transaction has a value of at least $100.00.

DETAILED DISCUSSION OF THE REFERENCES

A. Burger (U.S. Patent 6,219,439 B1) discloses a biometric authentication system including a reader 12 for a "smart card" 14 embedded with a computer chip 20 having a select amount of memory 22 therein. The memory 22 includes system operation information 24, user information 26, and other system operation information 32 (see Figure 1). The user information 26 includes fingerprint memory 28 and identification information 30 (see Column 5, lines 29-

40). As noted in Column 4, lines 28-33, retina scan, voice identification, saliva, DNA, or other biometrics may be used instead of the fingerprint. The system is used for authenticating an individual carrying the smart card 14 by comparing the fingerprint information received directly from the individual with the fingerprint data stored in the chip memory 22. This authentication is done at the scene on board the reader 12, and not at a remote location (see Column 5, lines 57-58). Further, there is no communication to or from a remote location central processing unit or any other device for authentication (see Column 6, lines 1-4). In other words, there is no communication between the system 10 and any central remote location for authentication.

In contrast, in the claimed invention, the identifying biometric characteristic and the profile information obtained from the portable data device carried by the person, is compared with the corresponding identifying biometric characteristic and the profile information prestored collectively at a central location for a successful or unsuccessful comparison **(crosscheck)**. No such **crosscheck** is carried out in Burger.

Further, Burger requires the authentication (the first comparison) to be a prerequisite to a second comparison between the non-biometric identifier of the smart card and other user data stored remote from the smart card to further determine authentication status of the user (see Column 6, lines 39-67). No such precondition is present in the claimed invention.

Moreover, it is respectfully submitted that Burger fails to disclose the claimed step of determining an active or inactive status of the data device (see subparagraph i) of Claims 1 and 14, and subparagraph h) of Claim 17).

Finally, it is respectfully submitted that Burger fails to disclose the features of at least dependent Claims 2-4, 9-12, 15-16 and 20, as noted above.

B. Lewis (U.S. Patent 6,213,391 B1) discloses a portable personal identification system in the form of an enclosure 1 housing various components, including verifying means 2, code generator 5, storage medium 6, memory chip 7, and output ports 10, 11 and 15 (see Figure 1). An input 12 receives the user's analog voice representation, or iris scan, fingerprint scan, DNA or other characteristic unique to individuals (see Column 7, lines 54-59 and Column 7, line 66 to Column 8, line 7). The verifying means obtains any pre-stored authorized profiles associated with an account and then compares the stored profile to the potential user's spontaneously created profile. If the spontaneous profile calculated by verifying means 2 matches, or is within an acceptable discrepancy value range of any of the authorized profile stored in the built in storage medium 6, the verifying means 2 generates a "Positive ID" signal that is output at port 10 to be transmitted to a program, circuitry or other device associated therewith to grant or deny access to the secured objective (see Column 8, lines 8-35 and Column 10, lines 1-23).

The system disclosed in Lewis operates to identify a card holder as an authorized or unauthorized user by converting the user's spontaneous word or phrase into a voice print value and comparing it with the predetermined ID profile stored on the card, the online computer database, or both, for match or discrepancy range (see Column 4, lines 58-67).

However, it is respectfully submitted that Lewis does not compare the identifying biometric characteristic and the profile information stored on the portable data device (carried by the person wishing to negotiate a transaction) with the corresponding identifying biometric characteristic and the profile information prestored collectively at a central location (see subparagraph f) of Claims 1 and 14, and subparagraph g) of Claim 17). In other words, Lewis merely compares the potential user's spontaneously created profile with that of a stored profile to grant or deny access, and does not carry out a **crosscheck** as in the present invention.

Moreover, Lewis does not determine the active or inactive status of the data device carried by the person, or notifies an appropriate authority if the status of the data device is determined to be inactive (see subparagraphs i) and k) of Claims 1 and 14, and subparagraph h) of Claim 17).

Finally, it is respectfully submitted that Lewis fails to disclose the features of at least dependent Claims 2-4, 9-12, 15-16 and 20, as noted above.

C. Bradney et al. (U.S. Patent 6,208,264 B1) discloses a personal identification system 10 including a remote access control terminal or identification authentication unit 12. The terminal 12 receives a variety of inputs from a keyboard 16, a swipe-card unit or identification card reader 18, a fingerprint sensor 20, and a card key encoding data unit 22. A card key 32 (Figures 3-5) is encoded at a central processing facility with a unique code which represents the fingerprint of the cardholder. The system verifies a person's identity on site at the point-of-transaction (see Column 7, lines 24-27). A scan mirror 77 (Figure 5) simultaneously scans the coded memory 66, which includes the fingerprint identification information of the owner of the card key, account number, biographical data and encryption information specific to the card key (Column 6, lines 5-10) with the thumbprint of the user. If a match occurs between the card key (coded memory 66) and the thumbprint, the transaction is cleared for further processing (see Column 6, lines 40-47). **If** the information does not match, the read data is checked against the data stored in the centralized data and processing unit 14 to verify that the scan process at the point-of-sale is operating satisfactorily (see Column 9, lines 10-33). Should the information scanned from the customer's card still does not match with the print data, the merchant at his option, may seize the customer's credit card in contemplation of further investigation or otherwise terminate the transaction (see Column 9, lines 33-37).

It is respectfully submitted that Bradney et al. also do not require a **crosscheck** by comparing the identifying biometric characteristic and the profile

information stored on the portable data device carried by a person with the corresponding identifying biometric characteristic and the profile information prestored collectively at a central location (see subparagraph f) of Claims 1 and 14, and subparagraph g) of Claim 17).

Moreover, Bradney et al. do not determine an active or inactive status of the data device and notify an appropriate authority if the status of the data device is determined to be inactive (see subparagraphs i) and k) of Claims 1 and 14, and subparagraph h) of Claim 17).

Finally, it is respectfully submitted that Bradney et al. fail to disclose the features of at least dependent Claims 2-4, 9-12, 15-16 and 20, as noted above.

D. Piosenka et al. (U.S. Patent 4, 993,068) discloses a personal identification system for identifying users at remote access control sites. The system utilizes immutable physical traits, such as facial photograph, retinal pattern, fingerprints, or handprints, voice pattern and static or dynamic personal signatures, to prove that the bearer of the credentials is indeed the person for whom the credentials were generated (see Column 3, lines 34-48). The credentials are issued in the form of a credit card-sized card containing identification credentials (see Column 4, line 61 to Column 5, line 19). The user 2 presents his credentials 4 to a credentials reader 35 for identification purposes. One or more of the physical traits are input by user 2 for comparison. The result of the comparison is the decision that the user 2 is physically the same individual

as that described on the media card 3 (see Column 8, lines 58-61). If the comparison is positive, the access control interface would open a door or gate, for example (see Column 8, lines 67-68).

However, it is submitted that Piosenka et al.'s system operates autonomously from the authorization site. In other words, for each user presenting himself to the verification site, a message is not sent to the centralized database of the authorization site (see Column 10, lines 12-27). Therefore, Piosenka et al. also do not carry out a **crosscheck** by comparing the identifying biometric characteristic and the profile information obtained directly from the portable data device with the corresponding identifying biometric characteristic and the profile information prestored collectively at a central location for a successful or unsuccessful comparison (see subparagraph f) of Claims 1 and 14, and subparagraph g) of Claim 17).

Moreover, Piosenka et al. do not determine an active or inactive status of the data device carried by the person and notify an appropriate authority if the status of the data device is determined to be inactive (see subparagraph i) and k) of Claims 1 and 14, and subparagraph h) of Claim 17).

Finally, it is respectfully submitted that Piosenka et al. fail to disclose the features of at least dependent Claims 2-4, 9-12, 15-16 and 20, as noted above.

E. Ware (U.S. Patent 4,707,592) discloses a personal universal identity card system, which includes a card reader 12 for receiving and reading a card 13, and transmitting the code and other data via a modem 24 and a data link 26 to a transaction center 11. The card reader 12 is connected to a computer 14 that operates to control the functions of the card reader 12. The card 13 includes an invisible, but machine-readable stripe that contains encoding, such as laser imprinting, barcode or an imbedded chip, or a card-code that may be combined with the user supplied personal code not present on the card to verify the card-carrying person's account or identity (see Column 2, lines 34-40). The central transaction center receives the card code and the personal code and other transaction information to determine whether or not the records indicate that the user's account is in good standing (see Column 2, lines 45-58).

The main function of the Ware's system is to prevent fraudulent or unauthorized use of cards by a system that avoids the use of paper with information that can be misused at the place of a transaction, etc.

When conducting a transaction, the user's identity is confirmed by having the user input his personal code or authorized code that is verified at the central computer to check to see if he is in good standing.

Although Ware states that the integrity of the system can be improved by adding additional personal identifying information data to the card, such as signature, voiceprint or a thumbprint, which is compared with corresponding data in the card holder's file in the transaction center (see Column 12, lines 22-32), the

system, nonetheless, requires the use of a personal or authorized code. No such requirement is present in the claimed invention. Therefore, Ware's system operates in a completely different manner than the claimed invention.

Moreover, Ware's system does not determine an active or inactive status of the data device carried by the person and does not notify an appropriate authority if the status of the data device is determined to be inactive (see subparagraphs i) and k) of Claims 1 and 14, and subparagraph h) of Claim 17).

Finally, it is respectfully submitted that Ware fails to disclose the features of at least dependent Claims 2-4, 9-12, 15-16 and 20, as noted above.

In view of the foregoing, it is respectfully submitted that Claims 1-20 are not anticipated by Burger, Lewis, Bradney et al., Piosenka et al. or Ware.

F. In addition to the above, it is respectfully submitted that there is no teaching or suggestion in Burger, Lewis, Bradney et al., Piosenka et al. and Ware that would have motivated one of ordinary skill in the art to combine the teachings thereof to render the claimed invention obvious.

G. Finally, it is respectfully submitted that Claims 1-20 are neither anticipated by nor obvious over the remaining references of record.

CONCLUSION

For the foregoing reasons, it is respectfully submitted that Claims 1-20 are patentable over the art of record. Therefore, it is respectfully requested that the above-identified application be accelerated for examination purposes.

It is believed that no additional fee is due for this submission. Should that determination be incorrect, however, the Commissioner is hereby authorized to charge any deficiencies, or credit any overpayment, to our Deposit Account No. 01-0433, and notify the undersigned in due course.

Should the Examiner have any questions or wish to discuss further this matter, please contact the undersigned at the telephone number provided below.

Respectfully submitted,

DINESH AGARWAL
Attorney for Applicant(s)
Reg. No. 31,809

Law Office - Dinesh Agarwal, P.C.
5350 Shawnee Road, Suite 330
Alexandria, Virginia 22312
Telephone: (703) 642-9400
Fax: (703) 642-9402

DA/mm